Before the
National Telecommunications and Information Administration
Washington, DC 20230

In the Matter of	)	
	)	
Public Notice on Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct	)	Docket No. 120214135-2135-01

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Danielle Coffey
Vice President & General Counsel, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

April 2, 2012

Table of Contents

Executive Summary

TIA member companies support the objectives outlined in the recently released White House Consumer Privacy Bill of Rights ("White House Framework"), as an important blueprint for assuring public confidence in the digital marketplace. As consumers express concerns about the collection of their personal data without their knowledge and the use of this information, protections should provide users with the necessary tools to enforce their individual preferences. The ICT industry recognizes the importance of consumer privacy concerns and has a strong interest in ensuring that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services. TIA believes that a significant benefit to consumers of the digital economy is the opportunity to use information about customers' needs and interests to create and offer personalized products and services. Policy solutions should not limit an individual consumer's choice to choose the appropriate balance between privacy and these innovations that provide convenience, speed or easier communication. TIA applauds the White House effort for attempting to strike an appropriate balance among these competing interests.

The use of consumer information to design products and improve services, as well as to fund free services and content, has produced substantial benefits for consumers. Americans are accustomed to making pragmatic choices about their privacy in our information economy. Networked technologies and the collection of data allow for consumers to have a much more personalized experience and to engage in "automated dialogue" about their needs and interests. Additionally, many online services and mobile applications are offered online free of charge, but collect some type of information from the user, perhaps age, sex and general location. Consumers need to be given more credit for understanding their choices in opting for convenience. The White House Framework preferences expressed on the principles of "Respect for Context" and "Focused Collection" needs to be balanced with preference of many consumers for personal customization. Regulations that greatly hinder the availability of information and implement burdensome technical safeguards would be costly to consumers in the form of less availability of free services and content and more expensive more expensive products.

Industry understands that if consumers do not trust that new technologies and business models will respect their privacy preferences or keep their sensitive information secure, users will be hesitant to use such technologies. They are also well positioned to understand providers' technological and business needs and to propose privacy protective solutions that offer an effective sector-wide response while allowing market and technical innovations to continue. As a result, industry self-regulation has been found to be a powerful tool for use in developing appropriate privacy norms. Since the early period of the internet's popularity, ICT industry members have been very aggressive in recognizing emerging concerns about privacy and taking steps to institute self-regulated models. These efforts have been very successful and indicate industry's continued commitment to ensuring consumer privacy and enhancing their trust in the ICT marketplace without the need for strong government regulation. TIA members are strongly committed to providing their customers with an environment that discourages fraud and promotes pro-customer behavior.

There is no single source of privacy law in the U.S. Existing privacy laws have generally focused on regulating the use of sensitive information, rather than attempting to dictate how consumer records are maintained. The U.S. model has attempted to recognize that individuals have varying levels of concern about the privacy depending on the type of information and the context in which it is or could potentially be used. There is an extensive body of state and federal law to safeguard consumer privacy covering a range of things from health, financial, and children's records. Our national approach of focusing on the areas of greatest concern reflects a careful balancing of consumer interests. The prospects for comprehensive privacy legislation are beyond the scope of this proceeding. However, the multistakeholder process that NTIA recommends should be informed by attention to the existing legal framework for privacy and great care should be taken to avoid attempts to comprehensively develop rules for how private organizations maintain and use customer data.

The White House Framework does not distinguish between "online" and "brick and mortar" privacy in addressing marketing practices. TIA applauds the White House for taking an approach that is technology neutral. The focus of privacy protection should be on how information is used, collected, and safeguarded, not on which technology is used for those functions. Technological convergence has made legal and regulatory distinctions between "networked" and "brick and

mortar" consumer relationships irrelevant. Regulations based on invalid distinctions can fail in their purpose and do real economic harm by discouraging the adoption of network technologies.

Industry has strong incentives to protect consumer information, particularly sensitive consumer information, and thus self-regulation has been an effective complement to governmental action, particularly for new and evolving technologies. As a standards development organization, TIA notes that the ICT industry has a history of successful standards collaboration. We encourage NTIA to hold an Issue Identification workshop specifically focused on process so that all stakeholders are able to further discuss their views regarding scope, timelines, and procedures for moving forward.

The White House Framework calls for a regulation of consumer "personal data" that is broader than any previous U.S. legislation. Trying to regulate such a broad scope of data is fraught with challenges. Unique identifiers pose a particularly vexing problem if subject to privacy regulations. Unique identifiers are present and used in nearly every consumer product or service and at nearly every level of the distribution chain. Without consensus on the scope of data within the ambit of any code of conduct, industry will struggle as to when to trigger the code of conduct. TIA recommends that prior to drafting any codes of conduct, further discussion is needed to seek agreement on the privacy principles outlined in the White House Report and in particular the scope of data subject to the principles.

In order to focus on meeting consumer expectations for privacy protections, TIA believes that, as a useful framework for analysis, privacy proposals under consideration at NTIA should be measured against the yardstick of the following four tests:

- Are consumers empowered to apply their individual privacy preferences?
- Are privacy proposal requirements technology-neutral?
- Do privacy proposal requirements promote uniformity?
- Do privacy proposal requirements contain proportionate penalties?

I. Introduction

The Telecommunications Industry Association ("TIA") hereby submits comments to the National Telecommunications and Information Administration ("NTIA") in the above-captioned proceeding.

TIA, on behalf of its members, appreciates the importance of the interplay between information privacy and innovation in the Internet economy. TIA believes that an appropriate privacy framework balances consumer privacy concerns with the consumer benefits arising from technological innovation and business model flexibility in communications and Internet commerce. Thus, as explained below, TIA supports the privacy framework now in place in the United States, which focuses on notice, choice, appropriate data protection, and robust enforcement. To the extent that additional protections are required, NTIA should work to facilitate the expansion of self-regulatory regimes, which have already proven successful in structuring providers' conduct, rather than supporting new prescriptive requirements, which would threaten innovation and undermine consumer welfare. Moreover, any modifications to the existing privacy framework must be technology-neutral, focusing on how information is used and protected, rather than the specific means by which it is collected and used.

TIA represents the global information and communications technology ("ICT") industry through standards development, advocacy, trade shows, business opportunities, market intelligence and world-wide environmental regulatory analysis. Its member companies manufacture or supply the products and services used in the provision of broadband and broadband-enabled applications. Since 1924, TIA has enhanced the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications. Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment.

II. Discussion

A. TIA Members Support Privacy Protections for Users.

1. TIA Members Support the White House Consumer Privacy Bill of Rights' Objectives

The TIA member companies strongly concur with the objectives of the White House Consumer Privacy Bill of Rights ("White House Framework")[1] It furnishes an important blueprint for assuring public confidence in the digital marketplace. Many consumers are concerned that their personal data may be collected without their knowledge, used in a way they do not expect or desire, or misused to invade their privacy. Privacy protections should provide users with the necessary tools to enforce their individual preferences about what information will be collected and how it will be used.

TIA believes that a significant benefit of the digital economy for consumers is served by the opportunity to use information about customers' needs and interests to create and offer personalized products and services.. Policies ought not to limit an individual consumer's own choices, which may favor such innovations that provide convenience, speed or easier communication.

Yet as the ability to collect, use, and store information about consumers has increased, so has consumer concerns about privacy. It is in the interest of the ICT industry to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information in exchange for benefits such as greater convenience, increased safety, or enhanced communications.

As explained below, TIA supports the privacy framework now in place in the United States, which focuses on notice, choice, appropriate data protection, and proportionate penalties. Privacy protections should not dictate which technologies may be used, as long as consumers receive appropriate notice and can exercise choice about how these technologies collect, use, and share their information.

[1] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 10, February 2012.

TIA applauds the White House effort for attempting to strike an appropriate balance among these competing interests.

B. Consumers Benefit from the Pace of Technology Innovation

1. Technological Innovation Results in Greater Consumer Choice and Significant Benefits, including Access to Personalization

The use of consumer information to design products and improve services, as well as to fund free services and content, has produced substantial benefits for consumers.

Americans are accustomed to making pragmatic choices about their privacy in our information economy. As consumers, we can choose to pay in cash to preserve our anonymity. But we regularly choose to give information about ourselves. We know that credit card purchases produce a "paper trail" of information about our lifestyle and other characteristics. We also know that by ordering products through a mail order catalog, we will get future offers for related products. Consumers need to be given more credit for understanding their choices when they opt for convenience.

Networked technologies are, in fact, seeking to duplicate the same personalized attention that consumers get from the best brick and mortar merchants. A traditional merchant often knows based upon past experience, or even conjecture, to be able to make recommendations. Consumers value the personal attention that this requires.

In many respects, the interactive nature of networked communication is far more similar to a conversation with a brick & mortar merchant than it is with more conventional mass media electronic medium. Not only can the consumer reject the merchant's recommendations, but also he can guide the dialogue in a direction that results in a more mutually satisfactory conclusion. Online processes that replicate familiarity with consumer preferences are a positive characteristic of online commerce

The personalization of consumer communications to customize consumer contact and engage the consumer in an "automated dialogue" is a benefit of the Internet. Sophisticated retention of past buying patterns and other data can help a marketer personalize their contact with a customer. The

openness and communications power of the Internet provides strong incentives for e-commerce companies to keep their customers satisfied. For example, search engines and other related tools compete with each other in their ability to identify and access desired content. Regulators have noted the consumer benefit that of marketing personalization. [2]

The White House Framework preferences expressed on the principles of "Respect for Context" and "Focused Collection" needs to be balanced with the preference of many consumers for personal customization.

Many online services and mobile applications are offered online free of charge, but collect some type of information from the user, perhaps age, sex and general location. While some advocates dwell on one particular type of technology or service as posing a drastic threat to consumers' privacy, these fears are often hypothetical only and do not take into account new consumer benefits. Individual consumers are best suited to determine if future offers have been tailored to fit their specific interest.

Privacy regulations that greatly hinder the availability of information would be costly to consumers, who would receive fewer of the resulting benefits, such as improved services and products and greater convenience.

For example, free services and content may become less widely available or suffer a reduction in quality because a critical source of their funding — targeted advertising—may become less valuable. Also, onerous restrictions on behavioral advertising would likely increase the volume of unwanted marketing messages. Finally, if members of the ICT industry are required to implement burdensome technical safeguards as part of their product specifications, the costs will

[2] *See, e.g.*, Jon Leibowitz, Chairman, Fed. Trade Commission, Keynote Address at the National Cable & Telecommunications Association Cable Show 2010 (May 12, 2010) (stating that targeted advertising is "usually good for consumers, who don't have to waste their time slogging through pitches for products they would never buy; good for advertisers, who efficiently reach their customers; and good for the Internet, where online advertising helps support the free content everyone enjoys and expects"); *see also* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 112 (2008) ("It is not obvious, however, that better information about consumer behavior increases the amount of marketing. It clearly leads to more targeted have concerns, however, about how their data is collected, stored, and used.").

invariably be passed on to consumers, which will likely raise the price of new products and thereby deter adoption.

2. Consumer demand already encourages the adoption of "privacy best practices."

Industry understands that if consumers do not trust that new technologies and business models will respect their privacy preferences or keep their sensitive information secure, users will be hesitant to use such technologies. Consumer mistrust of new products and services slows consumer adoption. Consequently, the ICT industry wants to ensure that consumers have sufficient confidence about their privacy so that they are willing to embrace new technologies and services and, based on their preferences, to share their information to receive benefits such as greater convenience, increased safety, or enhanced communications.

Industry members are necessarily sensitive to consumers' demands. They are also well positioned to understand providers' technological and business needs and to propose privacy protective solutions that offer an effective sector-wide response while allowing market and technical innovations to continue. Given the providers' interest in marrying strong privacy protections with consumer choice and innovation, self-regulatory regimes are a powerful tool for use in developing appropriate privacy norms. As the White House Framework acknowledges, existing voluntary self-regulation privacy initiatives have already substantially contributed fostering consumer confidence. Future efforts offer greater flexibility in responding promptly to new concerns to better meet emerging threats.

Consumers have embraced new technologies and business models that provide improved capabilities and greater value. For example, all of the applications and services that are the subject of self-regulation discussed below – mobile marketing, targeted advertising, and location based wireless services– offer consumers enormous benefits. These include improved personal safety and security through easy access to maps and directions and the ability to locate children and friends through location-based services; more efficient shopping and searches through advertising that is better targeted to the recipient's interests; and savings and convenience through offers such as mobile coupons provided through mobile marketing. There are also innovative business models that use consumer information to support an array of new goods and

services, often provided to consumers free of charge. For example, search engines give users access to a universe of information at speeds and scales that were previously unimaginable. In addition to benefits to individual consumers, the collection of data in anonymized form can provide societal benefits, such as epidemic detection and other medical insights, or improvements in urban planning.

Competitive pressures encourage the adoption of "privacy best practices" in order to assure consumer confidence. Companies that fail to meet consumer expectations can expect the word to spread quickly, much more quickly than in more traditional vendor/customer environments. TIA members are strongly committed to providing their customers with an environment that discourages fraud and promotes pro-customer behavior.

Consumer surveys demonstrate that consumers are already carefully weighing the impact on their privacy. Regulators should not place unnecessary barriers to offering consumers convenience, nor should they underestimate the capacity of consumers to make informed choices. Innovation has also increased the amount of control consumers can exercise over their personal information.

Accordingly, the ICT industry has participated in a variety of self-regulatory efforts to address privacy concerns and enhance consumer confidence in new technologies and business models. Since the early period of the internet's popularity, industry members have been very aggressive in recognizing emerging concerns about privacy and taking steps to institute self-regulated models.

1. At the outset of the internet, consumers were cautious about using it, particularly for commercial activities. The Online Privacy Alliance formed in 1998 by a coalition of global companies and trade associations with the intent of fostering consumer trust and protection of their online privacy. The Alliance promoted guidelines that led to the adoption of effective Internet privacy policies by the private sector.[3] It also developed a framework for enforcing consumer privacy that called for objective third party monitoring of website compliance with privacy policies and provision of a mechanism for consumer complaint and resolution.

[3] Online Privacy Alliance, http://www.privacyalliance.org/ (last visited March 30, 2012).

2. Shortly after that, in 2000, the Network Advertising Initiative was formed to address concerns about online advertisers' use of cookies to track consumers' web browsing in order to facilitate behavioral advertising.[4] The founding companies of NAI worked with the Federal Trade Commission to develop a self-regulatory framework to provide notice and mechanisms for alter the scope of the data tracking including opt out systems.[5] NAI continues to operate today and has updated its code of conduct and tracks compliance among its member organizations.

Within the relatively short period in which mobile application have been a feature of the consumer wireless market, several industry led initiative have addressed specific consumer concerns:

1. Mobile Marketing Association Code of Conduct. For example, many TIA members follow the Mobile Marketing Association Code of Conduct, which requires companies to provide consumers notice about how their information will be used; choice (based on obtaining customer consent, offering customization by consumers, and requiring constraint by marketers); and security for consumer information.[6]

2. Self-Regulatory Principles for Online Behavioral Advertising. TIA Members have also participated in the development of the cross-industry Self-Regulatory Principles for Online Behavioral Advertising issued by the Better Business Bureau and leading advertising industry associations. [7] The Principles aim to provide consumers greater transparency, choice, and control regarding the collection and use of their information for online behavioral advertising purposes. The Digital Advertising Alliance (DAA), a consortium of advertising trade groups, announced plans to expand consumer choice on privacy. The DAA plans to include a "do not track" button on web browsers that the organization's members would honor. [8] DAA members already support a privacy icon to

[4] *See* Network Advertising Alliance, History, http://www.networkadvertising.org/about/history.asp (last visited March 30, 2012).
[5] *See id.*
[6] Mobile Mktg. Ass'n, Code of Conduct (July 2008), http://mmaglobal.com/policies/code-of-conduct (last visited March 29, 2012).
[7] Internet Advertising Board, Self-Regulatory Principles for Online Behavioral Advertising (July 2009), *available at* http://www.iab.net/public_policy/behavioral-advertisingprinciples
[8] *See* The Self-Regulatory Program for Online Behavioral Advertising,

give consumers the opportunity to opt out of ads.[9]

3. Best Practices and Guidelines for Location- Based Services. In addition, CTIA has also promulgated Best Practices and Guidelines for Location- Based Services, which are based on the fundamental principles of user notice and consent regarding their location information and which aim to facilitate consumer use of new and exciting location-based services.[10] CTIA Best Practices and Guidelines ("Guidelines") are intended to promote and protect user privacy as new and exciting Location-Based Services ("LBS") are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the Guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.). The Guidelines rely on two fundamental principles: user notice and consent.[11]

4. Mobile Application Rating System. CTIA and the Entertainment Software Rating Board (ESRB) announced in November 2011 that they have developed a rating system that mobile application storefronts voluntarily support as part of their application submission (or onboarding) process. The CTIA Mobile Application Rating System with ESRB uses the familiar age rating icons that ESRB assigns to computer and video games to provide parents and consumers reliable information about the age-appropriateness of applications. [12]

5. Mobile Privacy Principles. CTIA members have also worked on privacy matters through the GSM Association's (GSMA) Mobile Privacy Initiative, which published principles

---

Digital Advertising Alliance Position On Browser Based Choice Mechanism, https://www.aboutads.info/resource/download/DAA_Commitment.pdf.

[9] The Self-Regulatory Program for Online Behavioral Advertising, Opt Out from Online Behavioral Advertising, http://www.aboutads.info/choices/

[10] CTIA Business Resources, Best Practices and Guidelines for Location-Based Services, http://www.ctia.org/business_resources/wic/index.cfm/AID/11300 (last visited March 30, 2012).

[11] *Id*. *http://www.ctia.org/business_resources/wic/index.cfm/AID/11300*

[12] CTIA, *CTIA-The Wireless Association and ESRB Announce Mobile Application Rating System* (Nov. 29, 2011), http://www.ctia.org/media/press/body.cfm/prid/2147

regarding notice, transparency, and control for consumers over information that is collected or accessed by mobile applications. In February, they released privacy guidelines to provide for more functional and coordinated implementation of the principles across mobile platforms.[13]

6. Also, the leading mobile platform providers agreed to abide by stricter privacy policies at the behest of the California Attorney General.[14] As part of the agreement, the companies will give customers the option to read the privacy policy before downloading a new or updated mobile application. These companies also agreed to provide a means for customers to report apps that don't comply with terms of service.

These efforts indicate industry's continued commitment to ensuring consumer privacy and enhancing their trust in the ICT marketplace without the need for strong government regulation. A key factor to the continued success of these self-regulatory initiatives was the ability to target it to the relevant industry players that have a stake in effective outcomes.

C. Existing Privacy Rules Focus on Areas of Greatest Consumer Concern

There is no single source of privacy law in the U.S. Existing privacy laws have generally focused on regulating the use of sensitive information, rather than attempting to dictate how consumer records are maintained. Our national approach of focusing on the areas of greatest concern reflects a careful balancing of consumer interests. Beyond the restraint that consumers exercise in the use of personally identifiable information, there are numerous state and Federal laws that govern its use. This includes laws affecting financial, health and children's information.

There is an extensive body of state and federal law to safeguard consumer privacy, including Section 5 of the Federal Trade Commission Act. This provides a strong but flexible privacy

---

[13] Jennifer Baker, *Mobile Network Operators Set Guidelines for App Privacy*, PC WORLD (Feb 27, 2012 11:40 am), http://www.pcworld.com/businesscenter/article/250773/mobile_network_operators_set_guidelines_for_app_privacy.html.

[14] State of Cal., Office of Attorney Gen., Mobile Applications and the Mobile Privacy Fact Sheet, *available at* http://ag.ca.gov/cms_attachments/press/pdfs/n2630_updated_mobile_apps_info.pdf.

framework based on consumer notice and choice, as well as reasonable security measures to protect consumers' personal information from unauthorized access or release. Certain types of information are subject to additional protections, such as those set out in the Communications Act of 1934, as Amended ("Communications Act") and the Health Insurance Portability and Accountability Act ("HIPAA"). By accounting for consumer demands, sensitivity of information, and other relevant factors, this existing framework has proven effective in addressing privacy challenges arising from innovations in information use and technology. [15]

Existing law, such Fair Credit Reporting legislation, gives consumers access to those that might result in adverse decisions. These processes also give consumers the opportunity to amend their records with clarifying information. Widely accepted industry privacy self-regulation standards already exist. The Federal Trade Commission has encouraged these efforts and has the Sec. 5 power enforce them**.**

The prospects for comprehensive privacy legislation are beyond the scope of this proceeding. However the multistakeholder process that NTIA recommends should be informed by attention to the existing legal framework for privacy, which focuses specific users concerns about the potential misuse of personal information. Care should be taken to avoid attempts to comprehensively develop rules for how private organizations maintain and use customer data.

---

[15] *Some of the relevant laws include: [1] Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D(Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954) This Act directs the FTC to issue a rule requiring entities that obtain consumers' personal information but are not subject to the Health Insurance Portability & Accountability Act ("HIPAA") (Pub. L. No. 104-191, 110 Stat. 1936 (1996)), [2] The Fair Credit Reporting Act (FCRA) is a United States federal law (codified at 15 U.S.C. § 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information.* The FTC, (Federal Trade Commission Act, 15 U.S.C. § 45) provides general oversight for much of the collection, use, and sharing of consumer information for most businesses through application of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The FTC's longstanding approach rests primarily on efforts to ensure (1) that consumers are afforded notice of what marketing -- there is a higher probability that the consumer will find the message relevant if information about past behavior helps to predict preferences."). 2 See Fed. Trade Commission Staff Report, Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology, at 1 (Feb. 2009), available *at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (discussing consumer concerns over personal data collection). [3] The Federal Communications Commission ("FCC") administers Consumer Proprietary Network 5. Information ("CPNI") regulations See 47 U.S.C. § 222 (establishing duty of every telecommunications carrier to protect confidentiality of customers' CPNI).*

D. Privacy Regulation Should be Technology Neutral.

The White House Consumer Data Privacy Framework does not distinguish between "online" and "brick and mortar" privacy in addressing marketing practices.

As noted above, the current privacy framework is based on providing the consumer notice about what information is collected and how it will be used, choice about whether to provide personal information, and security for the personal information that is collected.

Technological convergence has made legal and regulatory distinctions between "networked" and "brick and mortar" consumer relationships irrelevant. Regulations based on invalid distinctions can fail in their purpose and do real economic harm by discouraging the adoption of network technologies

The framework is based on the consumer's expectations about how his or her personal information will be treated, not the technologies being used.

The focus of privacy protection should be on how information is used, collected, and safeguarded, not on which technology is used for those functions. For example, if a consumer chooses to provide personal information online pursuant to a privacy policy that promises that such information will not be shared with third parties for marketing purposes, it matters little to the consumer if the privacy promise is broken through a cookie that collects the information as he types it in, through a technology that intercepts the message while it is traveling over the network, or through the later release of that information from the recipient's database. Privacy protection should focus on how information is used and protected, rather than the means of information collection, whether it is through cookies, deep packet inspection, or paper records.

It is notable that the FTC's recent series of cases addressing failures to maintain personal information securely did not differentiate based on the technology used to safeguard the information. The FTC brought actions against companies that failed to secure their networks, as well as against a drug store chain that disposed of pill bottles with sensitive medical information by throwing them into the trash. The focus was properly on the violation of the privacy

protections promised to consumers, not on which technology was used to collect or store the consumer information.

E. NTIA Can Draw Upon the Experience from Successful Codes of Conduct Development

1. Existing Voluntary, Consensus- Based Processes Can Advance Conduct Codes

Industry has strong incentives to protect consumer information, particularly sensitive consumer information, and thus self-regulation has been an effective complement to governmental action, particularly for new and evolving technologies.

As noted above examples of self-regulation include the Mobile Marketing Association Code of Conduct, the Better Business Bureau Self-Regulatory Principles for Online Behavioral Advertising, and CTIA-The Wireless Association Best Practices and Guidelines for Location-Based Services. Industry members are well positioned to understand technological and business needs and to propose solutions that protect consumer privacy while allowing market and technical innovations to continue.

NTIA asks about how to create a consensus based process. Also already noted above there are a number of successful industry conduct codes. As a standards development organization, TIA notes that the ICT industry has a history of successful standards collaboration. We note that the American National Standards process incorporates broadly applicable processes: [16]

- consensus by a group that is open to representatives from all interested parties
- broad-based public review and comment on draft standards
- consideration of and response to comments
- incorporation of submitted changes that meet the same consensus requirements into a draft standard

[16] American National Standards Institute, OVERVIEW OF THE U.S. STANDARDIZATION SYSTEM: Voluntary Consensus Standards and Conformity Assessment Activities, 2007; also see OMB CIRCULAR NO. A-119 Revised, http://www.whitehouse.gov/omb/circulars_a119#2

- availability of an appeal by any participant alleging that these principles were not respected during the standards-development process.

We note that consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.

We encourage NTIA to hold an Issue Identification workshop specifically focused on process so that all stakeholders are able to further discuss their views regarding scope, timelines, and procedures for moving forward.

2. TIA recommends that prior to drafting any codes of conduct, further discussion is needed to seek agreement on the privacy principles outlined in the White House Report and in particular the scope of data subject to the principles.

While TIA supports the concept that industry is best positioned to address the implementation of agreed-upon privacy principles, without consensus on the foundation upon which the Codes of Conduct will be built, any Code of Conduct cannot stand. Never before has U.S. legislation attempted to regulate consumer "personal data" defined so broadly as to include, "any data, including aggregations of data, which is linkable to a specific individual . . . [including] an identifier on a smartphone or family computer that is used to build a usage profile . . ." (Report at p. 10).

The "law" of unintended consequences weighs heavily on any decision on the breadth of information subject to any code of conduct. Trying to regulate such a broad scope of data is fraught with challenges. For example, the EU cookie directive has been widely criticized, has not been implemented into law by the majority of EU member states, and has proven exceedingly impractical for business to implement.

Unique identifiers pose a particularly vexing problem if subject to privacy regulations. Unique identifiers are present and used in nearly every consumer product or service and at nearly every

level of the distribution chain. They are used in everything from the VIN number on cars, to the codes on our food items and medicines, to the dozens of unique identifiers within mobile phones including hardware, firmware, software, and service unique identifiers. Without consensus on the scope of data within the ambit of any code of conduct, industry will struggle as to when to trigger the code of conduct.

3. TIA Recommends NTIA consider privacy protection proposals against the yardstick of the following four tests

Effective privacy protections are important for consumers and the ICT industry, particularly in an era of rapid technological change. Consumers will only adopt new information and communications technologies if they trust that their personal privacy preferences will be respected and that their personal information will remain secure. Innovations in information use and technology, coupled with effective privacy protections, have greatly enriched consumer choices and experiences and benefitted our economy.

In order to focus on meeting consumer expectations for privacy protections, TIA believes that, as a useful framework for analysis, privacy proposals under consideration at NTIA should be measured against the yardstick of the following four tests:

a) Are consumers empowered to apply their individual privacy preferences?

To the maximum extent possible, consumers should be empowered to make their own privacy choices. Individual privacy preferences vary greatly; so tools are necessary to address the many variations of individual preference.

TIA members support this framework of notice, choice, and security. Consumers should be able to access clear descriptions of the types of personal data collected and the purpose for which that data is being used and to exercise choice about whether to permit their personal information to be collected and used as described. In addition, any company that collects and maintains such information must take reasonable security measures to guard against unauthorized access to it.

Beyond notice, though, technological tools can users enforce their preference on a systematic basis.

b) Are privacy proposal requirements technology neutral?

TIA members believe that consumer expectations focus on information's sensitivity, not the technology being used. Rules for privacy, especially in a marketing context, should not change depending upon the medium used to collect information. Drawing distinctions between "online" information and other marketing data gathered in a more "traditional" setting is inconsistent with consumer expectations that their personal information is all part of a single relationship with a merchant.

c) Do privacy proposal requirements promote uniformity?

In general, consumer expectations are that rules are consistent. In a networked economy, the exchange of information is an essential component to commerce. Voluntary industry codes of conducts can foster consumer expectations for the treatment of their personally identifiable information. The interests of the Constitution's Commerce Clause are served by having uniform privacy enforcement rules. As the White House Framework notes, industry codes of conduct can offer this benefit.

d) ***Do privacy proposal requirements contain proportionate penalties***?

Consumer expectations are that violators will face enforcement with penalties that are proportionate to actual consequences. TIA members believe that existing law enforcement tools give policymakers necessary tools to punish bad actors.

The willingness of industry to <u>voluntarily</u> commit to privacy codes of conduct depends in part on a reasonable enforcement process that does not excessively penalize in excess of actual harm. TIA members acknowledge the constructive role that the Federal Trade Commission has in data privacy protection.

III. CONCLUSION

Appropriate collection, sharing, and use of consumer information provide many benefits to industry, the economy, and consumers. It is thus vitally important that privacy protections maintain flexibility for different business models and technologies to ensure that these benefits continue. Businesses may collect and use information to provide more convenient services or to improve products or customer service. Information about consumers may also be used for marketing purposes, which permits more targeted marketing and also underwrites the provision of free content and services on the Internet and other channels thereby making services more affordable for all consumers.

For the foregoing reasons, TIA urges NTIA to take into consideration its views in this proceeding.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President & General Counsel, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

April 2, 2012